CURTEA DE CONTURI EUROPEANĂ

Decizia nr. 041-2021 a Curții de Conturi Europene privind normele de securitate pentru protecția informațiilor UE clasificate (IUEC)

CURTEA DE CONTURI EUROPEANĂ,

AVÂND ÎN VEDERE articolul 13 din Tratatul privind Uniunea Europeană,

AVÂND ÎN VEDERE articolul 287 din Tratatul privind funcționarea Uniunii Europene,

AVÂND ÎN VEDERE articolul 257 din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii,

AVÂND ÎN VEDERE articolul 1 alineatul (6) din normele de aplicare a Regulamentului de procedură al Curții de Conturi (Decizia nr. 21-2021 a Curții de Conturi Europene),

AVÂND ÎN VEDERE normele de securitate pentru protecția informațiilor UE clasificate ale celorlalte instituții, agenții și organe ale UE,

AVÂND ÎN VEDERE politica Curții de Conturi Europene privind securitatea informațiilor (DEC/127/15 FINAL) și politica privind clasificarea informațiilor (Comunicarea către personal nr. 123/2020),

ÎNTRUCÂT în temeiul articolului 287 alineatul (3) din TFUE, Curtea de Conturi Europeană are dreptul de a accesa toate documentele relevante și toate informațiile necesare, din punctul său de vedere, pentru a-și exercita mandatul, inclusiv informații UE clasificate (IUEC), iar acest drept trebuie să fie exercitat cu respectarea deplină a principiului cooperării sincere între instituții și a principiului atribuirii competențelor; întrucât dreptul de acces la IUEC, garantat prin TFUE, nu poate fi contestat de sursa IUEC și întrucât Curții de Conturi Europene i se poate solicita să instituie și să respecte anumite măsuri de securitate, după cum se detaliază în cele ce urmează;

ÎNTRUCÂT membrii Curții de Conturi Europene, funcționarii acesteia și alți membri ai personalului trebuie să respecte, chiar și după părăsirea locului de muncă, obligația de confidențialitate prevăzută la articolul 339 din TFUE, la articolul 17 din Statutul funcționarilor și în alte acte adoptate în temeiul acestor instrumente;

ÎNTRUCÂT având în vedere caracterul sensibil al acestora, gestionarea IUEC impune respectarea obligației de confidențialitate, care se va asigura prin măsuri de securitate corespunzătoare capabile să garanteze un nivel ridicat de protecție pentru informațiile respective și echivalente cu cele stabilite prin normele privind protecția IUEC adoptate de alte instituții, agenții și organe ale UE, înțelegându-se că, în cazul în care Curtea de Conturi Europeană consideră că orice astfel de măsuri de securitate nu se justifică ținând cont de natura și de

tipul IUEC, aceasta își rezervă dreptul de a prezenta orice observații pe care le consideră necesare, respectând totodată nivelul de clasificare al IUEC;

ÎNTRUCÂT măsurile de securitate pentru protejarea confidențialității, a integrității și a disponibilității informațiilor comunicate Curții de Conturi Europene trebuie să fie adecvate tipului și naturii informațiilor în cauză;

ÎNTRUCÂT Curții de Conturi Europene trebuie să i se acorde accesul la informații clasificate, în conformitate cu principiul necesității de a cunoaște, în vederea desfășurării sarcinilor încredințate prin tratate și prin acte juridice adoptate pe baza tratatelor;

ÎNTRUCÂT având în vedere natura și caracterul sensibil al anumitor informații, este adecvat să se instituie o procedură specială pentru gestionarea de către Curtea de Conturi Europeană a documentelor care conțin IUEC;

ÎNTRUCÂT instituția trebuie să se asigure că prezenta decizie este pusă în aplicare în conformitate cu toate normele aplicabile, în special cu dispozițiile referitoare la protecția datelor cu caracter personal, la securitatea fizică a persoanelor, a clădirilor și a echipamentelor IT și la accesul public la documente;

DECIDE:

Articolul 1. Obiect și domeniu de aplicare

(1) Prezenta decizie stabilește principiile de bază și standardele minime de securitate pentru protecția informațiilor clasificate gestionate de Curtea de Conturi Europeană în exercitarea mandatului său.

(2) În scopurile prezentei decizii, informații clasificate înseamnă oricare dintre următoarele tipuri de informații sau toate:

(a) „informații UE clasificate” (IUEC), astfel cum sunt definite în normele de securitate ale altor instituții, agenții, organe sau oficii ale UE și care poartă unul dintre următoarele marcaje de clasificare de securitate:

- TRÈS SECRET UE/EU TOP SECRET: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii deosebit de grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- SECRET UE/EU SECRET: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- CONFIDENTIEL UE/EU CONFIDENTIAL: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- RESTREINT UE/EU RESTRICTED informații și materiale a căror divulgare neautorizată ar putea fi în defavoarea intereselor Uniunii Europene sau ale unuia ori mai multor state membre.

(b) informațiile clasificate furnizate de către statele membre și pe care figurează un marcaj de clasificare de securitate național echivalent cu unul dintre marcajele de clasificare de securitate utilizate pentru IUEC[1], enumerate la litera (a);

(c) informațiile clasificate furnizate Curții de Conturi Europene de state terțe sau de organizații internaționale și care poartă un marcaj de clasificare de securitate echivalent cu unul dintre marcajele utilizate pentru IUEC și enumerate la litera (a), în conformitate cu acordurile privind securitatea informațiilor sau cu acordurile administrative relevante.

(3) Curtea de Conturi Europeană gestionează informațiile de nivel RESTREINT UE/EU RESTRICTED în incinta sa și ia toate măsurile de protecție necesare în acest scop. Se iau măsurile necesare pentru ca personalul Curții de Conturi Europene care are nevoie să acceseze IUEC de un nivel mai ridicat să facă acest lucru în incinte adecvate ale altor instituții, organe sau agenții ale UE.

(4) Prezenta decizie se aplică tuturor serviciilor din cadrul Curții de Conturi Europene și în ansamblu incintelor acesteia.

(5) Cu excepția dispozițiilor care se aplică doar anumitor categorii de personal, prezenta decizie se aplică membrilor Curții de Conturi Europene, personalului Curții de Conturi Europene care intră în domeniul de aplicare al Statutului funcționarilor și Regimului aplicabil celorlalți agenți ai Uniunii Europene[2], experților naționali detașați pe lângă Curtea de Conturi Europeană, furnizorilor de servicii și angajaților acestora, stagiarilor și tuturor persoanelor cărora le este permis accesul în clădirile Curții de Conturi Europene sau la alte bunuri ale acesteia ori accesul la informațiile tratate de Curtea de Conturi Europeană.

(6) În lipsa unor dispoziții contrare, dispozițiile referitoare la IUEC se aplică într-o manieră echivalentă și informațiilor clasificate menționate la alineatul (2) literele (b) și (c) de la prezentul articol.

Articolul 2. **Definiții**

În sensul prezentei decizii:

(a) „autorizație de acces la IUEC” înseamnă o decizie a directorului Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene, luată pe baza unei asigurări date de o autoritate competentă a unui stat membru, conform căreia unui funcționar, unui alt agent al Curții de Conturi Europene sau unui expert național detașat, odată ce s-a stabilit că este necesar ca persoana în cauză să aibă cunoștință de astfel de informații și cu condiția ca aceasta să fi fost informată corespunzător cu privire la responsabilitățile sale, îi poate fi acordat accesul la IUEC până la un nivel de clasificare precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) și până la o anumită dată; se consideră că persoana astfel descrisă deține „autorizația de securitate”;

(b) „clasificare” înseamnă atribuirea unui nivel de clasificare unei anumite informații, în funcție de gradul de prejudiciu care ar putea fi provocat de dezvăluirea sa neautorizată;

---

[1] A se vedea Acordul din 4 mai 2011 dintre statele membre ale Uniunii Europene, reunite în cadrul Consiliului, privind protecția informațiilor clasificate schimbate în interesul Uniunii Europene și anexa la acesta (JO 2011/C 202/13).

[2] Regulamentul nr. 31 (CEE) de stabilire a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți ai Uniunii Europene, astfel cum a fost modificat, JO 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31(1)/2020-01-01).

(c) „material criptografic” înseamnă algoritmi criptografici, module criptografice hardware și software și produse însoțite de detalii de instalare și documentația aferentă, precum și materialul de criptare;

(d) „declasificare” înseamnă eliminarea oricărei clasificări de securitate;

(e) „document” înseamnă orice informație înregistrată, indiferent de forma sau de caracteristicile sale fizice;

(f) „reducerea nivelului de securitate” înseamnă atribuirea unui nivel de clasificare inferior;

(g) „autorizare de securitate industrială” înseamnă o decizie administrativă a unei autorități de securitate competente conform căreia, în ceea ce privește securitatea, un obiectiv poate oferi un nivel de protecție adecvat pentru IUEC clasificate la un anumit nivel de clasificare a securității;

(h) „gestionarea” IUEC înseamnă toate acțiunile posibile al căror obiect îl pot face IUEC de-a lungul ciclului lor de viață: creare, înregistrare, prelucrare, transport, reducerea nivelului de clasificare, declasificare și distrugere. În ceea ce privește sistemele informatice și de comunicații (SIC), gestionarea cuprinde, de asemenea, colectarea, afișarea, transmiterea și păstrarea;

(i) „deținător” înseamnă o persoană autorizată în mod corespunzător, în privința căreia s-a stabilit necesitatea de a cunoaște, care se află în posesia unei informații clasificate și, în consecință, răspunde de protecția acesteia;

(j) „autoritatea pentru securitatea informațiilor” înseamnă responsabilul pentru securitatea informațiilor din cadrul Curții de Conturi Europene, care poate delega integral sau parțial atribuțiile prevăzute în prezenta decizie;

(k) „informație” înseamnă orice informație scrisă sau orală, oricare ar fi suportul sau autorul acesteia;

(l) „material” înseamnă orice suport, mediu de stocare a datelor sau orice aparat ori echipament;

(m) „emitent” înseamnă o instituție, un organ sau o agenție a Uniunii, un stat membru, un stat terț sau o organizație internațională sub a cărei autoritate s-au creat și/sau introdus informațiile în structurile UE;

(n) „acordarea autorizării de securitate personalului” (ASP) înseamnă o declarație a unei autorități competente a unui stat membru făcută după finalizarea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru, care certifică faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) și până la o anumită dată, cu condiția să se fi stabilit necesitatea de a cunoaște în cazul său și ca persoana în cauză să fi fost informată în mod corespunzător cu privire la responsabilitățile sale;

(o) „certificare a autorizării de securitate a personalului” (CASP) înseamnă un certificat eliberat de directorul Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene, care stabilește că o persoană deține un certificat de securitate valabil sau o autorizare de securitate și care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), perioada de valabilitate a certificatului sau a autorizării de securitate corespunzătoare și data expirării certificatului în cauză;

(p) „autoritatea pentru securitatea fizică” înseamnă responsabilul de securitate din cadrul Curții de Conturi Europene, care răspunde de punerea în aplicare a măsurilor și procedurilor de securitate fizică necesare pentru protejarea IUEC;

(q) „Biroul de ținere a evidenței” este administrat de secretariatul Curții și este situat într-o zonă administrativă aflată sub răspunderea directorului Direcției Resurse umane, finanțe

și servicii generale a Curții de Conturi Europene. Acesta este responsabil pentru intrarea și ieșirea informațiilor RESTREINT UE/EU RESTRICTED sau cu un nivel echivalent care sunt comunicate către Curtea de Conturi Europeană;

(r) „Registratura IUEC" este o entitate creată în interiorul unei zone securizate. Aceasta este gestionată de responsabilul de control al registraturii din cadrul Curții de Conturi Europene, care deține autorizarea de securitate necesară. Acesta este responsabil pentru intrarea și ieșirea informațiilor CONFIDENTIEL UE/EU CONFIDENTIAL sau cu un nivel echivalent ori superior care sunt comunicate către Curtea de Conturi Europeană.

(s) „autoritatea de acreditare în materie de securitate" (AAS) înseamnă directorul Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene.

Articolul 3. **Măsuri pentru protecția IUEC**

(1) Curtea de Conturi Europeană asigură protecția tuturor informațiilor clasificate ce îi sunt furnizate, într-o manieră proporțională cu nivelul de clasificare stabilit de emitent și în conformitate cu prezenta decizie.

(2) În acest scop, Curtea de Conturi Europeană condiționează gestionarea IUEC de măsuri de securitate fizică și, acolo unde este cazul, de măsuri de securitate privind personalul, inclusiv de existența autorizațiilor de acces pentru persoanele identificate și a măsurilor pentru protecția sistemelor informatice și de comunicații. Aceste măsuri sunt descrise la articolele 4-6 și se aplică pe parcursul întregului ciclu de viață al IUEC. Ele trebuie să fie proporționale cu clasificarea de securitate a IUEC, cu forma și volumul informațiilor sau ale materialelor, cu amplasarea și construcția spațiilor în care sunt păstrate IUEC și cu evaluarea locală a amenințării reprezentate de activități rău-intenționate și/sau infracționale, inclusiv spionaj, sabotaj și terorism.

(3) IUEC sunt protejate prin măsuri de securitate fizică, iar informațiile clasificate drept CONFIDENTIEL UE/EU CONFIDENTIAL sau cu un nivel superior sunt protejate, în plus, prin măsuri de securitate privind personalul.

(4) IUEC pot fi furnizate doar persoanelor care au nevoie să le cunoască din cadrul instituției. Deținătorul oricărei IUEC trebuie să protejeze informația respectivă în conformitate cu dispozițiile prezentei decizii.

(5) IUEC nu trebuie divulgate verbal sau în scris. Observațiile preliminare, rapoartele, avizele, comunicatele de presă și alte produse ale Curții de Conturi Europene, site-ul său web și rețeaua intranet, intervențiile orale, răspunsurile la solicitările de acces la documente[3] și înregistrările audio sau video nu trebuie să conțină IUEC sau extrase din acestea ori să facă referire la ele. Totuși, dacă emitentul a publicat documente sau informații care conțin o trimitere la IUEC, se poate menționa referința respectivă.

(6) Fără a aduce atingere dispozițiilor de la alineatul (5), Curtea de Conturi Europeană și emitentul pot conveni ca, în cazul unui anumit audit, Curtea de Conturi Europeană să poată reproduce sau folosi elemente ale IUEC într-un document. Într-o astfel de situație, documentul Curții de Conturi Europene este transmis mai întâi emitentului IUEC în cauză, înainte de procedura contradictorie sau în timpul acesteia. Curtea de Conturi Europeană și emitentul stabilesc în acest caz dacă documentul emis de Curtea de Conturi Europeană se clasifică. În cazul în care

[3] În temeiul Deciziei nr. 12-2005 a Curții de Conturi Europene privind accesul public la documentele Curții de Conturi, astfel cum a fost modificată prin Decizia nr. 14-2009 (JO 2009/C 67/1).

un membru raportor al Curții de Conturi Europene consideră necesară comunicarea unui raport de audit clasificat integral sau parțial către anumiți destinatari din cadrul Parlamentului European sau al Consiliului – ținând cont de toate măsurile de securitate asociate prezentei decizii – acesta trebuie să obțină aprobarea emitentului informațiilor clasificate. Cadrul juridic și procedura pentru schimbul de astfel de documente sunt prevăzute la articolul 7.

(7) În cazul în care exercitarea mandatului său impune ca anumite elemente ale unui document sau ale unei informații clasificate să fie partajate pe scară mai largă, Curtea de Conturi Europeană, ținând cont în mod corespunzător de marcajul de clasificare de securitate, consultă emitentul înainte de a decide să folosească acele elemente sau informații, în cazul în care consideră că există un interes public superior în acest sens. Informațiile pot fi utilizate în raport doar de așa manieră încât să nu se aducă atingere interesului emitentului. Acest lucru poate fi garantat în mod corespunzător solicitându-i emitentului să transmită observații pentru a se ajunge la un acord cu privire la modalitatea de anonimizare, condensare sau generalizare a informațiilor etc., respectându-se în același timp interesele celor vizați în principal de informațiile publicate.

(8) Curtea de Conturi Europeană nu furnizează IUEC altei instituții, agenții, organ sau oficiu al UE, unui stat membru, unui stat terț sau unei organizații internaționale fără consultarea prealabilă și consimțământul scris explicit al emitentului.

(9) Cu excepția cazului în care emitentul unui document clasificat la nivelul SECRET UE/EU SECRET sau la un nivel inferior a impus restricții privind duplicarea sau traducerea acestuia, documentele respective pot fi duplicate sau traduse la solicitarea deținătorului și în conformitate cu instrucțiunile practice de lucru ale autorității pentru securitatea informațiilor din cadrul Curții de Conturi Europene. Măsurile de securitate aplicabile documentului original se aplică, de asemenea, copiilor și traducerilor acestuia.

(10) În cazul în care are nevoie de reducerea nivelului de securitate sau de declasificarea unui document clasificat pe care l-a primit sau pe care este autorizată să îl acceseze, Curtea de Conturi Europeană îl consultă pe emitent pentru a întreba dacă acesta poate pune la dispoziție o versiune a documentului care să fie declasificată sau care să aibă un nivel de securitate mai redus.

Articolul 4. Măsuri de securitate privind personalul

(1) În virtutea funcțiilor pe care le ocupă, membrii Curții de Conturi Europene sunt autorizați să aibă acces la toate IUEC și să participe la întâlniri în cadrul cărora se gestionează IUEC. Membrii sunt informați cu privire la obligațiile lor în materie de securitate în ceea ce privește protecția IUEC și își asumă în scris răspunderea pentru protejarea acestor informații.

(2) Un membru al personalului Curții de Conturi Europene, indiferent dacă este funcționar, dacă face obiectul Regimului aplicabil celorlalți agenți ai Uniunii Europene sau este expert național detașat, primește acces la IUEC doar după ce:

i. a fost stabilită în cazul său necesitatea de a cunoaște;

ii. a fost informat cu privire la normele de securitate pentru protecția IUEC și cu privire la standardele și orientările relevante în materie de securitate și a confirmat în scris că a luat cunoștință de responsabilitățile care îi revin cu privire la protecția informațiilor de acest tip; și

iii. în cazul informațiilor clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, a primit autorizarea de securitate și i s-a acordat autorizația de acces.

(3) Procedura pentru a determina măsura în care un funcționar sau alt membru al personalului Curții de Conturi Europene poate fi autorizat să acceseze informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, ținându-se cont de loialitatea, integritatea și credibilitatea persoanei și după obținerea asigurării din partea autorităților competente ale unui stat membru, astfel cum se prevede la articolul 2 litera (n), se stabilește într-o decizie delegată adoptată în temeiul articolului 10 alineatul (10). Deciziile de a acorda autorizația de acces sunt adoptate de directorul Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene.

(4) Directorul Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene poate emite CASP în care specifică nivelul de clasificare pentru care li se poate acorda persoanelor respective acces la IUEC (nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau un nivel superior), perioada de valabilitate a autorizației de acces corespunzătoare și data expirării CASP.

(5) Doar persoanele cu autorizația menționată la alineatul (2) punctul (iii) de mai sus și membrii Curții de Conturi Europene, în temeiul alineatului (1) de mai sus, pot participa la întâlniri în care sunt gestionate informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior. Curtea de Conturi Europeană și emitentul iau măsurile necesare pentru organizarea acestor întâlniri, în funcție de situație.

(6) Serviciile din cadrul Curții de Conturi Europene care sunt responsabile pentru organizarea de întâlniri în cadrul cărora se vor gestiona informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior informează în timp util autoritatea pentru securitatea informațiilor cu privire la datele, orele și locurile întâlnirilor și furnizează listele de participanți.

(7) Orice persoană care se află în posesia IUEC fără autorizația corespunzătoare și/sau fără o nevoie demonstrată de a le cunoaște trebuie să raporteze cât mai curând posibil situația autorității pentru securitatea informațiilor și să se asigure că IUEC sunt protejate conform dispozițiilor prezentei decizii.

Articolul 5. Măsuri de securitate fizică pentru protejarea informațiilor clasificate

(1) „Securitate fizică” înseamnă utilizarea măsurilor de protecție fizică și tehnică pentru a împiedica accesul neautorizat la IUEC.

(2) Măsurile de securitate fizică sunt concepute astfel încât să împiedice accesul disimulat sau forțat al vreunui intrus, să descurajeze, să împiedice și să detecteze acțiunile neautorizate și să permită stabilirea unei distincții între membrii personalului în ceea ce privește accesul acestora la IUEC, pe baza principiului necesității de a cunoaște. Aceste măsuri sunt stabilite pe baza unei proceduri de gestionare a riscurilor, în conformitate cu prezenta decizie.

(3) Spațiile unde sunt gestionate sau păstrate IUEC sunt supuse unor inspecții periodice ale autorității de securitate competente din cadrul Curții de Conturi Europene.

(4) Pentru gestionarea și stocarea IUEC se folosesc doar echipamente sau dispozitive care respectă normele aplicabile în cadrul instituțiilor, agențiilor sau organelor UE pentru protejarea IUEC.

(5) Personalul Curții de Conturi Europene poate accesa IUEC clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior ori informații echivalente în zone securizate din afara incintelor Curții de Conturi Europene.

(6) Curtea de Conturi Europeană poate încheia un acord privind nivelul serviciilor cu o altă instituție a UE din Luxemburg pentru a putea gestiona și stoca informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior într-o zonă securizată a instituției respective. Cu excepția cazului în care emitentul și-a dat acordul în mod explicit asupra acestui aspect, aceste IUEC nu sunt gestionate sau stocate în incintele Curții de Conturi Europene și nu pot fi duplicate sau traduse de aceasta.

(7) Informațiile RESTREINT UE/EU RESTRICTED care sunt primite sunt înregistrate de Curtea de Conturi Europeană. Consultarea informațiilor clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior ori a informațiilor echivalente în afara incintelor Curții de Conturi Europene trebuie să fie înregistrată în scopuri de securitate.

(8) IUEC clasificate la nivelul RESTREINT UE/EU RESTRICTED pot fi păstrate în mobilier de birou adaptat și încuiat, într-o zonă administrativă sau o zonă securizată. IUEC clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET se stochează în temeiul unui acord privind nivelul serviciilor într-un recipient securizat într-o zonă securizată a altei instituții a UE din Luxemburg.

(9) Atunci când se află în afara registraturii, IUEC sunt transferate între servicii și incinte după cum urmează:

(a) ca regulă generală, IUEC sunt transmise prin mijloace electronice protejate prin intermediul unor produse criptografice aprobate în conformitate cu articolul 6 alineatul (8);

(b) dacă nu sunt transmise după cum se descrie la litera (a), IUEC se transferă folosind un suport de date (de exemplu, stick de memorie USB, CD, hard disk) protejat prin produse criptografice aprobate în conformitate cu articolul 6 alineatul (8) sau pe hârtie, într-un plic opac și sigilat.

(10) Informațiile RESTREINT UE/EU RESTRICTED pot fi distruse de deținător, sub rezerva respectării normelor privind arhivarea aplicabile în cadrul Curții de Conturi Europene. Informațiile clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior pot fi distruse doar de responsabilul de control al registraturii, la instrucțiunile deținătorului sau ale unei autorități competente, în conformitate cu normele privind arhivarea aplicabile în cadrul Curții de Conturi Europene. Distrugerea documentelor clasificate la nivelul SECRET UE/EU SECRET se efectuează în prezența unui martor cu o autorizație de securitate care corespunde cel puțin nivelului de clasificare al documentului ce urmează să fie distrus. Responsabilul de control al registraturii și martorul, atunci când este necesară prezența acestuia, semnează un proces-verbal de distrugere, care este păstrat de registratură. Responsabilul de control al registraturii păstrează procesele-verbale de distrugere a documentelor CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET timp de cel puțin cinci ani.

(11) Autoritatea pentru securitatea fizică și autoritatea pentru securitatea informațiilor elaborează un plan comun, ținând cont de condițiile locale, pentru protejarea IUEC în perioade de criză, inclusiv, acolo unde este necesar, planuri pentru distrugerea sau evacuarea acestora în caz de urgență. Entitățile în cauză emit instrucțiunile pe care le consideră necesare pentru ca IUEC să nu parvină unor persoane neautorizate.

(12) Atunci când IUEC trebuie să fie transportate fizic, Curtea de Conturi Europeană respectă măsurile impuse de emitent pentru a le proteja împotriva dezvăluirii neautorizate în timpul transportului.

(13) Măsurile de securitate fizică ce se aplică în zonele administrative în care sunt gestionate și stocate informații RESTREINT UE/EU RESTRICTED sunt prevăzute în anexă.

Articolul 6. **Protejarea IUEC în cadrul sistemelor informatice și de comunicații**

(1) În sensul prezentului articol, „sistem informatic și de comunicații” înseamnă orice sistem care permite gestionarea IUEC în format electronic. Un sistem informatic și de comunicații cuprinde toate mijloacele necesare pentru funcționarea sa, inclusiv infrastructura, organizarea, personalul și resursele informaționale.

(2) „Utilizator legitim” înseamnă un membru al Curții de Conturi Europene, un funcționar, alt membru al personalului sau un expert național detașat cu nevoia stabilită și recunoscută de a accesa un anumit sistem informatic.

(3) Curtea de Conturi Europeană garantează că sistemele sale vor proteja informațiile gestionate într-o măsură adecvată și vor funcționa așa cum trebuie, când trebuie, sub controlul utilizatorilor legitimi. În acest scop, acestea garantează niveluri adecvate de:

- autenticitate: garanția faptului că informațiile sunt veridice și provin de la surse de bună credință;
- disponibilitate: proprietatea informațiilor de a putea fi accesate și utilizate la cerere de către o entitate autorizată;
- confidențialitate: proprietatea informațiilor de a nu fi divulgate persoanelor, entităților sau proceselor neautorizate;
- integritate: proprietate care constă în garantarea acurateței și a exhaustivității activelor și a informațiilor;
- nerepudiere: capacitatea de a dovedi că o acțiune sau un eveniment a avut loc, astfel încât acțiunea sau evenimentul în cauză să nu poată fi negate ulterior.

Aceste garanții se bazează pe un proces de gestionare a riscurilor. „Risc” înseamnă posibilitatea ca o anumită amenințare să exploateze vulnerabilitățile interne și externe ale unei organizații sau ale oricăruia dintre sistemele pe care aceasta le utilizează și, în consecință, să cauzeze un prejudiciu organizației sau activelor sale corporale ori necorporale. Riscul se măsoară ținându-se cont, în același timp, de probabilitatea materializării amenințărilor și de impactul acestora. Procesul de gestionare a riscurilor constă în următoarele etape: identificarea amenințărilor și a vulnerabilităților, evaluarea riscurilor, tratarea riscurilor, acceptarea riscurilor și comunicarea riscurilor.

- „Evaluarea riscului” constă în identificarea amenințărilor și a vulnerabilităților și în desfășurarea analizei de risc aferente, și anume evaluarea probabilității și a impactului.
- „Tratarea riscului” constă în atenuarea, eliminarea sau reducerea riscului (printr-o combinație adecvată de măsuri de ordin tehnic, fizic, organizațional sau procedural), transferul riscului sau monitorizarea acestuia.
- „Acceptarea riscului” înseamnă decizia de a accepta, după tratarea riscului, existența în continuare a unui risc rezidual.
- „Risc rezidual” înseamnă riscul care persistă după punerea în aplicare a măsurilor de securitate, ținând seama de faptul că nu toate amenințările pot fi contracarate și nu toate vulnerabilitățile pot fi eliminate.
- „Comunicarea riscului” constă în sensibilizarea comunității de utilizatori ai sistemului informatic și de comunicații cu privire la riscuri, în informarea autorităților de omologare cu privire la aceste riscuri și în raportarea lor către autoritățile operaționale.

(4) Toate dispozitivele și echipamentele electronice folosite pentru gestionarea IUEC respectă normele aplicabile pentru protecția IUEC. Se acordă prioritate dispozitivelor și echipamentelor electronice care au fost deja acreditate de altă instituție, agenție sau organ al UE. Securitatea dispozitivelor se garantează pe parcursul întregului lor ciclu de viață.

(5) Sistemul informatic și de comunicații al Curții de Conturi Europene pentru gestionarea IUEC este acreditat de o autoritate adecvată. În acest scop, Curtea de Conturi Europeană încheie un

acord privind nivelul serviciilor cu o autoritate de acreditare în materie de securitate a unei instituții a UE care are capacitatea de a acredita SIC ce gestionează IUEC, în vederea primirii unei declarații de acreditare pentru gestionarea de informații RESTREINT UE/EU RESTRICTED prin SIC al Curții de Conturi Europene, precum și clauzele și condițiile de funcționare aferente. Acest acord privind nivelul serviciilor se referă și la standardele care se aplică procesului de acreditare și se încheie în conformitate cu procedura prevăzută la articolul 10 alineatul (3).

(6) În cazul în care Curtea de Conturi Europeană trebuie să își stabilească propriul proces de acreditare pentru SIC, procesul se instituie printr-o decizie delegată, astfel cum se menționează la articolul 10 alineatul (10) din prezenta decizie, în conformitate cu standardele privind procesul de acreditare pentru SIC care gestionează IUEC în alte instituții, agenții și organe ale UE.

(7) Responsabilitatea pentru pregătirea dosarelor de acreditare și a documentației în conformitate cu standardele aplicabile îi revine exclusiv proprietarului de sistem al SIC.

(8) În cazul în care IUEC sunt protejate prin produse criptografice, Curtea de Conturi acordă prioritate produselor aprobate de Consiliu sau de secretarul general al Consiliului, în calitatea sa de autoritate de aprobare criptografică, sau celor aprobate de alte instituții, agenții și organe ale UE pentru protecția IUEC.

(9) Informațiile RESTREINT UE/EU RESTRICTED se gestionează doar pe dispozitive electronice (precum stații de lucru, imprimante, copiatoare) care se află într-o zonă administrativă sau într-o zonă securizată. Dispozitivele electronice care gestionează informații RESTREINT UE/EU RESTRICTED sunt separate față de alte rețele informatice și sunt protejate prin măsuri fizice sau tehnice adecvate.

(10) Toți membrii personalului Curții de Conturi Europene implicați în proiectarea, dezvoltarea, testarea, funcționarea, gestionarea sau utilizarea unui SIC care tratează IUEC aduc la cunoștința responsabilului cu securitatea informațiilor toate posibilele deficiențe în materie de securitate, incidente, cazuri de încălcare sau de compromitere a securității care pot avea un impact asupra protecției SIC și/sau a IUEC pe care le conține acesta.

<u>Articolul 7.</u> Procedura pentru schimbul de informații clasificate și pentru permiterea accesului la acestea

(1) În cazul în care au obligația legală de a face acest lucru în temeiul tratatelor sau al actelor juridice adoptate pe baza tratatelor, instituțiile, agențiile, organele și oficiile UE și autoritățile naționale acordă acces Curții de Conturi Europene la IUEC cu respectarea procedurii de mai jos, din proprie inițiativă sau la solicitarea scrisă a președintelui, a unui membru raportor sau a secretarului general.

(2) Solicitările de acces se trimit instituțiilor în cauză prin intermediul Biroului de ținere a evidenței din cadrul Curții de Conturi Europene.

(3) Atunci când este necesar, Curtea de Conturi Europeană încheie un acord administrativ ce prevede dispoziții practice pentru schimbul de IUEC sau de informații echivalente.

(4) În scopul încheierii acestor acorduri administrative, Curtea de Conturi Europeană furnizează emitentului toate informațiile necesare cu privire la sistemul său de securitate a informațiilor. Dacă este nevoie, poate fi organizată o vizită de evaluare.

(5) Aceste acorduri administrative se încheie cu respectarea deplină a principiilor atribuirii competențelor și cooperării sincere prevăzute la articolul 13 din Tratatul privind Uniunea

Europeană. Acordurile se încheie în conformitate cu procedura prevăzută la articolul 10 alineatul (4).

(6) În cazul în care cu o anumită instituție, organ sau agenție a UE, cu un anumit stat terț sau cu o anumită organizație internațională nu există niciun acord administrativ cu privire la furnizarea de informații clasificate Curții de Conturi Europene, aceasta din urmă semnează o declarație prin care se angajează să protejeze informațiile clasificate pe care le primește.

Articolul 8. Încălcarea securității, pierderea sau compromiterea informațiilor clasificate

(1) O încălcare a securității înseamnă o faptă sau o omisiune a unei persoane care contravine normelor de securitate stabilite în prezenta decizie și în normele de punere în aplicare a acesteia.

(2) Compromiterea are loc atunci când, în urma unei încălcări a securității, IUEC au fost divulgate, integral sau parțial, unor persoane neautorizate.

(3) Orice încălcare sau suspiciune de încălcare a securității se raportează imediat autorității pentru securitatea informațiilor a Curții de Conturi Europene.

(4) Atunci când se știe sau există motive rezonabile pentru a se presupune că IUEC au fost compromise sau pierdute, autoritatea pentru securitatea informațiilor îi informează pe directorul Direcției Resurse umane, finanțe și servicii generale și pe secretarul general al Curții de Conturi Europene. Directorul Direcției Resurse umane, finanțe și servicii generale informează imediat autoritatea de securitate competentă a emitentului. Directorul sus-menționat efectuează o anchetă, informând secretarul general al Curții de Conturi Europene și autoritatea de securitate a emitentului cu privire la rezultate și la măsurile adoptate pentru a preveni repetarea situației. În cazurile care este vizat un membru al Curții de Conturi Europene, președintele instituției are obligația de a lua măsuri în cooperare cu secretarul general al acesteia.

(5) Orice funcționar sau alt membru al personalului Curții de Conturi Europene care se face responsabil de o încălcare a normelor de securitate prevăzute în prezenta decizie și în normele sale de punere în aplicare suportă sancțiunile prevăzute în Statutul funcționarilor și în Regimul aplicabil celorlalți agenți ai Uniunii Europene.

(6) Orice membru al Curții de Conturi Europene care nu respectă dispozițiile prezentei decizii se supune măsurilor și sancțiunilor prevăzute la articolul 286 alineatul (6) din tratat.

(7) Orice persoană responsabilă de pierderea sau compromiterea unor IUEC este pasibilă de acțiuni disciplinare și/sau în justiție, în conformitate cu actele cu putere de lege, normele și reglementările aplicabile.

Articolul 9. Securitatea în cazul unei intervenții externe

(1) În baza unui contract, Curtea de Conturi Europeană poate încredința îndeplinirea sarcinilor ce implică sau impun accesul la IUEC unor contractanți înregistrați într-un stat membru. Această situație poate apărea în special în legătură cu întreținerea sistemelor informatice și de comunicații și a rețelelor informatice.

(2) În cazul unei intervenții externe, Curtea de Conturi Europeană ia toate măsurile de securitate necesare menționate la alineatul (3) din prezentul articol, inclusiv solicitarea unei autorizări de securitate industrială, pentru a se asigura că IUEC sunt protejate de candidați și de ofertanți pe întreaga durată a unei proceduri de ofertare și de achiziție publică, precum și de către

contractanți și subcontractanți pe întreaga durată a contractului. Autoritatea contractantă veghează ca standardele minime de securitate prevăzute în prezenta decizie să fie menționate în contracte, astfel încât contractanții să fie obligați să le respecte.

(3) Normele de securitate, procedurile de achiziție publică și formularele și modelele pentru contractele și subcontractele care implică accesul la IUEC, anunțurile de participare, orientările privind circumstanțele în care este necesară autorizarea de securitate industrială și cea pentru personal, instrucțiunile de securitate pentru programe sau proiecte, anexe de securitate, vizitele și transmiterea și transportul IUEC în temeiul acestor contracte și subcontracte respectă normele, formularele și modelele stabilite de Comisia Europeană pentru contractele clasificate prin Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate.

Articolul 10. Punerea în aplicare a deciziei și responsabilitățile aferente

(1) Serviciile din cadrul Curții de Conturi Europene iau toate măsurile necesare care intră în sfera lor de responsabilitate pentru a se asigura că, atunci când gestionează sau păstrează IUEC sau orice alte informații clasificate, aplică prezenta decizie și normele de punere în aplicare relevante.

(2) Secretarul general este autoritatea împuternicită să facă numiri și autoritatea abilitată să încheie contracte de muncă pentru toți funcționarii și pentru alți membri ai personalului. Secretarul general poate delega directorului Direcției Resurse umane, finanțe și servicii generale responsabilitatea de a autoriza funcționarii și alți membri ai personalului să acceseze informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, de a exercita funcția de autoritate de acreditare în materie de securitate și de a supraveghea secretariatul Curții în ceea ce privește gestionarea IUEC.

(3) Secretarul general are competența de a încheia acorduri privind nivelul serviciilor în ceea ce privește acreditarea echipamentelor și sistemelor informatice și de comunicații ale Curții de Conturi Europene, utilizarea unei zone securizate dintr-o altă instituție a UE și procedura pentru solicitările de autorizare de securitate pentru personal în vederea obținerii accesului la IUEC.

(4) Directorul Direcției Resurse umane, finanțe și servicii generale are competența de a încheia cu instituțiile, agențiile și alte organe ale UE acorduri administrative vizând schimbul de IUEC de care Curtea de Conturi Europeană are nevoie pentru a-și îndeplini mandatul. Acest director poate încheia, de asemenea, cu țări terțe sau cu organizații internaționale acorduri administrative privind protejarea oricăror informații clasificate primite.

(5) Directorul Direcției Resurse umane, finanțe și servicii generale are competența de a semna orice declarație prin care se angajează la protejarea IUEC furnizate în contextul unei comunicări ad-hoc cu caracter excepțional.

(6) Responsabilul cu securitatea informațiilor din cadrul Curții de Conturi Europene îndeplinește funcția de autoritate pentru securitatea informațiilor. Responsabilul cu securitatea informațiilor și persoanele cărora acesta le deleagă integral sau parțial sarcinile sale dețin autorizarea de securitate corespunzătoare. Autoritatea pentru securitatea informațiilor își asumă responsabilitățile în strânsă cooperare cu Direcția Resurse umane, finanțe și servicii generale, cu Direcția Informare, locuri de muncă și inovare și cu Direcția Comitetului pentru controlul calității auditului (a se vedea în special articolele 4, 6 și 8). Autoritatea pentru securitatea informațiilor este, de asemenea, responsabilă pentru organizarea de întâlniri de formare și de sensibilizare cu privire la securitatea informațiilor și pentru efectuarea de inspecții periodice de verificare a respectării prezentei decizii, inclusiv în situația unor

intervenții externe, și pentru orice măsuri care trebuie adoptate pentru asigurarea conformității.

(7) Responsabilul de securitate poartă responsabilitatea pentru măsurile de securitate fizică (în special pentru cele prevăzute la articolul 5).

(8) Biroul de ținere a evidenței creat în cadrul secretariatului Curții este punctul de intrare și de ieșire pentru informațiile clasificate la nivelul RESTREINT UE/EU RESTRICTED care pot face obiectul schimburilor dintre Curtea de Conturi Europeană și alte instituții, agenții și organe ale UE sau statele membre. De asemenea, acesta este punctul de intrare și de ieșire pentru informațiile echivalente ale țărilor terțe și ale organizațiilor internaționale. Structura organizatorică a Biroului de ținere a evidenței se stabilește printr-o decizie delegată. Responsabilul cu evidențele are următoarele atribuții principale:

a) înregistrarea intrării și ieșirii informațiilor clasificate la nivelul RESTREINT UE/EU RESTRICTED;

b) managementul zonelor administrative dedicate pentru înregistrarea, gestionarea, stocarea și consultarea IUEC clasificate la nivelul RESTREINT UE/EU RESTRICTED.

(9) Se instituie o registratură, în temeiul unui acord privind nivelul serviciilor referitor la utilizarea zonei securizate a unei alte instituții a UE. Registratura organizată de secretariatul Curții sub responsabilitatea directorului Direcției Resurse umane, finanțe și servicii generale a Curții de Conturi Europene este punctul de intrare și de ieșire pentru informațiile clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior care pot face obiectul schimburilor dintre Curtea de Conturi Europeană și alte instituții, agenții și organe ale UE și statele membre. De asemenea, aceasta este punctul de intrare și de ieșire pentru informațiile echivalente ale țărilor terțe și ale organizațiilor internaționale. Registratura este dotată cu seifurile adecvate și cu alte echipamente de securitate corespunzătoare pentru protejarea informațiilor clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior. Modul de organizare a registraturii se stabilește printr-o decizie delegată. Responsabilul de control al registraturii trebuie să dețină autorizarea de securitate corespunzătoare și are următoarele atribuții principale:

(a) gestionarea operațiunilor legate de înregistrarea, consultarea, păstrarea, reproducerea, traducerea, transmiterea, expedierea și, după caz, distrugerea IUEC;

(b) îndeplinirea oricăror altor atribuții legate de protecția IUEC definite într-o decizie delegată.

(10) Comitetul administrativ adoptă o decizie delegată în care sunt prevăzute norme de punere în aplicare pentru prezenta decizie. Responsabilul cu securitatea informațiilor stabilește orientări privind securitatea informațiilor. Comitetul pentru controlul calității auditului elaborează orientări în materie de audit.

<u>Articolul 11.</u> **Intrarea în vigoare**

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Luxemburg, 3 iunie 2021.

Pentru Curtea de Conturi

Klaus-Heiner Lehne
Președinte

Anexă: MĂSURI DE SECURITATE FIZICĂ PRIVIND ZONELE ADMINISTRATIVE PENTRU IUEC

ANEXĂ

MĂSURI DE SECURITATE FIZICĂ PRIVIND ZONELE ADMINISTRATIVE PENTRU IUEC

(1) Prezenta anexă conține norme de punere în aplicare a articolului 5 din decizie. Acestea sunt norme minime pentru protecția fizică a zonelor administrative destinate informațiilor RESTREINT UE/EU RESTRICTED în cadrul Curții de Conturi Europene: zone desemnate pentru înregistrarea, stocarea și consultarea informațiilor clasificate la nivelul RESTREINT UE/EU RESTRICTED.

(2) Scopul măsurilor de securitate fizică din zonele administrative este de a preveni accesul neautorizat în acestea, după cum urmează:

(a) se instituie un perimetru delimitat în mod vizibil, care permite verificarea persoanelor;

(b) se permite accesul fără însoțitor doar pentru persoanele autorizate în mod corespunzător de autoritatea pentru securitatea informațiilor a Curții de Conturi sau de o altă autoritate competentă; și

(c) orice alte persoane trebuie să fie însoțite în permanență sau sunt supuse unor controale echivalente.

(3) Autoritatea pentru securitatea informațiilor din cadrul Curții de Conturi Europene poate acorda în mod excepțional acces unor persoane neautorizate, inclusiv pentru a desfășura activități într-o zonă administrativă, cu condiția ca aceasta să nu implice accesul la IUEC – care vor rămâne încuiate. Aceste persoane pot intra doar dacă sunt însoțite și sunt supravegheate în permanență de autoritatea pentru securitatea informațiilor sau de responsabilul de control al evidențelor.

(4) Autoritatea pentru securitatea informațiilor prevede proceduri pentru gestionarea cheilor și/sau a combinațiilor de cifruri pentru toate zonele administrative și obiectele de mobilier securizate. Scopul acestor proceduri este acela de a proteja împotriva accesului neautorizat.

(5) Combinațiile de cifruri sunt memorate de cel mai mic număr de persoane posibil care trebuie să le cunoască. Combinațiile de cifruri pentru obiectele de mobilier securizate folosite pentru stocarea informațiilor RESTREINT UE/EU RESTRICTED se schimbă:

- la primirea unui nou obiect de mobilier securizat;
- ori de câte ori se schimbă personalul care cunoaște cifrul;
- în cazul în care cifrul este sau se bănuiește că a fost compromis;
- în cazul în care una dintre încuietori a făcut obiectul unei operații de întreținere sau al unei reparații;
- cel puțin o dată la 12 luni.

(6) Autoritatea pentru securitatea informațiilor și responsabilul de securitate au obligația de a asigura respectarea acestor norme.